Docket No. 111325-040100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No. 3974
Xin WANG	)	Group Art Unit: 2135
Application No. 09/468,703	)	Examiner: Leynna A. Ha
Filed: December 21, 1999	)	
For: TRANSFERRING THE RIGHTS TO DECODE MESSAGES	)	Date: April 30, 2007

REQUEST FOR RECONSIDERATION

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action mailed October 31, 2006, Applicants respectfully request reconsideration and allowance of the application in view of the following remarks. Claims 1-15 and 18-33 are pending in this application, of which claims 1 and 15 are independent.

Claims 1, 4-7, 12-15, 19-21, 24-25, and 27-33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,084,969 to Wright et al. and U.S. 6,587,946 to Jakobsson. However, neither Wright nor Jakobsson, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 1, 4-7, 12-15, 19-21, 24-25, and 27-33.

For example, independent claim 1 recites, in relevant part, a method for encrypting an original message to be passed to a recipient by way of a grantor, the method comprising the steps of obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme; *generating a public proxy key based on a private key corresponding to the recipient and on the private key corresponding to said grantor*, wherein said grantor's private key and said recipient's private key are combined, and the combination

of the private keys is based on said public key encryption scheme and provides that it is computationally difficult to recover the recipient's private key from the public proxy key even with the knowledge of the grantor's private key; and applying the public proxy key to the encrypted message to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient and the available public key information, and wherein the encrypted message remains in an encrypted state while being transformed into the transformed message and is not decrypted to the original message and re-encrypted at any point during the transformation.

In addition, independent claim 15 recites, in relevant part, a method for encrypting an original message to be passed to a recipient by way of a grantor, the method comprising the steps of obtaining an encrypted message representative of the original message, the encrypted message having been encrypted with a public key corresponding to the grantor according to a public key encryption scheme; *generating a public proxy key based on a public key corresponding to the recipient and on the private key corresponding to the public key of said grantor*, wherein said grantor's private key and said recipient's public key are combined, and the combination of said grantor's private key and said recipient's public key is based on said public key encryption scheme; and applying the public proxy key to the encrypted message to transform the encrypted message into a transformed message, wherein the transformed message is decryptable by the recipient using information selected from the private key corresponding to the recipient's public key and the available public key information, and wherein the encrypted message remains in an encrypted state while being transformed into the transformed message and is not decrypted to the original message and re-encrypted at any point during the transformation.

Thus, claim 1 recites "generating a public proxy key based on a private key corresponding to the recipient and on the private key corresponding to said grantor" and claim 15 recites "generating a public proxy key based on a public key corresponding to the recipient and on the private key corresponding to the public key of said grantor." According to the present invention, a proxy key is a key that is used to transform a message encrypted for one recipient into a message encrypted for another recipient without decrypting the message in the process. The Examiner's attention is respectfully directed to page 23, lines

18-23, of the Specification which provides that a proxy encryption scheme is public if the "proxy keys it generates may be published without compromising its security and proxy transformations applied in untrusted environments; otherwise, the scheme is private. In a private scheme, when a proxy key is transferred from the grantor to the facilitator and grantee, care must be taken to protect the proxy key from disclosure. As a result, the proxy transformation which uses the proxy key must be performed in private as well." (Page 23, lines 18-23). At least these features are not disclosed, suggested, or rendered obvious by the teachings of Wright or Jakobsson, alone or in combination.

Instead, Wright merely discloses a way of using a proxy (server) to decrypt and re-encrypt a message. In this regard, the Examiner agrees that Wright fails to teach this fundamental feature of proxy encryption, that is, the proxy transformation of an encrypted message into a transformed message that "is not decrypted to the encrypted message and re-encrypted" as is required by the claims. Additionally, since the proxy in Wright uses an "old" private (session) key to decrypt and a "new" (session) key to re-encrypt a message, the (proxy) key information can not be communicated and disclosed to public and the re-encryption (or proxy) transformation can not be conducted in public. Accordingly, it is clear that Wright does not disclose or suggest "generating a public proxy key."

Similarly, contrary to the Examiner's assertions otherwise, Jakobsson also fails to disclose or suggest "generating a public proxy key." In particular, Jakobsson uses a quorum of proxy servers (as a proxy) to perform the proxy transformation and the (proxy) information for each proxy server to use is a share of the private key of the grantor (i.e., "the primary recipient"). Consequently, the (proxy) transformation conducted by the Jakobsson proxy servers cannot be carried out in public without compromising the security of the underlying scheme.

For at least the reasons stated above, neither Wright nor Jakobsson, taken alone or in combination, disclose, suggest, or render obvious, the invention recited in independent claims 1 and 15 under 35 U.S.C. § 103(a). Dependent claims 4-7, 12-14, 19-21, 24-25, and 27-33 are also allowable by virtue of their respective dependencies on claims 1 and 15, and also on their own merits. Therefore, Applicants respectfully request that the rejection of claims 1, 4-7, 12-15, 19-21, 24-25, and 27-33 under 35 U.S.C. § 103(a) in view of Wright and Jakobsson be reconsidered and withdrawn.

In addition, claims 2-3, 8-11, and 22-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright, Jakobsson, and U.S. Patent No. 5,748,736 to Mittra. However, none of Wright, Jakobsson, or Mittra, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 2-3, 8-11, and 22-23.

As is clearly presented above, neither Wright nor Jakobsson, taken alone or in combination, disclose, suggest, or render obvious the invention recited in independent claims 1 and 15. In this regard, Mittra also fails to overcome the deficiencies of Wright and Jokobsson with respect to claims 1 and 15.

Thus, for at least the reasons stated above, none of Wright, Jakobsson, or Mittra, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 1 and 15 under 35 U.S.C. § 103(a). Rejected dependent claims 2-3, 8-11, and 22-23 are also allowable by virtue of their respective dependencies on claims 1 and 15, and also on their own merits. Accordingly, Applicants respectfully request that the rejection of claims 2-3, 8-11, and 22-23 under 35 U.S.C. § 103(a) as being unpatentable over Wright, Jakobsson, and Mittra be reconsidered and withdrawn.

Claims 18 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wright, Jakobsson, and the article entitled Irish Times "Encryption Technology to Thwart Computer Hackers System Should Protect Security of E-Commerce" (City Edition). However, none of Wright, Jakobsson, or the Irish Times article, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 18 and 26.

As is clearly presented above, neither Wright nor Jakobsson, taken alone or in combination, disclose, suggest, or render obvious the invention recited in independent claims 1 and 15. In this regard, the Irish Times article also fails to overcome the deficiencies of Wright and Jokobsson with respect to claims 1 and 15.

Thus, for at least the reasons stated above, none of Wright, Jakobsson, or the Irish Times article, taken alone or in combination, disclose, suggest, or render obvious the invention recited in claims 1 and 15 under 35 U.S.C. § 103(a). Rejected dependent claims 18 and 26 are also allowable by virtue of their respective dependencies on claims 1 and 15, and also on their own merits. Accordingly, Applicants respectfully request that the rejection of

claims 18 and 26 under 35 U.S.C. § 103(a) as being unpatentable over Wright, Jakobsson, and the Irish Times article be reconsidered and withdrawn.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

In addition, if a new office action is deemed necessary by the Examiner in this case, Applicants respectfully request that the new office action be a non-final office action. In particular, Applicants did not receive a copy of the office action until three days immediately prior to the expiration of the extended period for reply. According to the Examiner, the office action was returned to the Office undelivered, and despite Applicants efforts to have the address of record changed, the Office neglected to send the office action to the proper address. Because of the failure of the Office to resend the office action to the correct address, Applicants did not have sufficient time to fully prepare a response. Therefore, Applicants submit that the next office action, if necessary, should be a non-final office action to give the Applicants a fair opportunity to reply.

Furthermore, Applicants believe that a new non-final office action is appropriate because the Examiner's rejections did not accurately reflect the language of the currently pending claims. In particular, the rejections of claims 1 and 15, in particular, asserted that Wright discloses "a public, non-communicative method for encrypting an original method to be passed to a recipient by way of a grantor" instead of the claimed "method for encrypting an original message to be passed to a recipient by way of a grantor." The limitations regarding the method being "public" and "non-communicative" are not consistent with the currently pending claims. As such, Applicants believe they are entitled to a new non-final office action that accurately reflects the language of the currently pending claims to ensure that the Examiner is fully considering the subject matter of the claimed invention.

Except for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required,

including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a **CONSTRUCTIVE PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

NIXON PEABODY, LLP

Date: April 30, 2007

/Stephen M. Hertzler, Reg. # 58,247/
Stephen M. Hertzler

Customer No.: 22204
NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, D.C. 20004-2128
(202) 585-8000